


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [e-mail](#)
 **Search Results**
**BROWSE****SEARCH****IEEE Xplore GUIDE**

Results for "((power analysis attack)&lt;in&gt;metadata)"

Your search matched 24 of 1424023 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.
 [e-mail](#)
» **Search Options**[View Session History](#)[New Search](#)» **Key**

Indicates full text access

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

**Modify Search**


 Check to search only within this results set
Display Format:  [Citation](#)  [Citation & Abstract](#)
 [Select All](#) [Deselect All](#)
 1. **Power analysis attacks and algorithmic approaches to their countermeasures in elliptic curve cryptosystems**

Hasan, M.A.;  
*Computers, IEEE Transactions on*  
 Volume 50, Issue 10, Oct. 2001 Page(s):1071 - 1083  
 Digital Object Identifier 10.1109/12.956092  
[Abstract](#) | Full Text: [PDF\(232 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)

 2. **A digital design flow for secure integrated circuits**

Tiri, K.; Verbauwheide, I.;  
*Computer-Aided Design of Integrated Circuits and Systems, IEEE Transaction on*  
 Volume 25, Issue 7, July 2006 Page(s):1197 - 1208  
 Digital Object Identifier 10.1109/TCAD.2005.855939  
[Abstract](#) | Full Text: [PDF\(528 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)

 3. **An overview of power analysis attacks against field programmable gate arrays**

Standaert, O.-X.; Peeters, E.; Rovroy, G.; Quisquater, J.-J.;  
*Proceedings of the IEEE*  
 Volume 94, Issue 2, Feb. 2006 Page(s):383 - 394  
 Digital Object Identifier 10.1109/JPROC.2005.862437  
[Abstract](#) | Full Text: [PDF\(472 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)

 4. **Examining smart-card security under the threat of power analysis attacks**

Messerges, T.S.; Dabbish, E.A.; Sloan, R.H.;  
*Computers, IEEE Transactions on*  
 Volume 51, Issue 5, May 2002 Page(s):541 - 552  
 Digital Object Identifier 10.1109/TC.2002.1004593  
[Abstract](#) | Full Text: [PDF\(400 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)

 5. **On the masking countermeasure and higher-order power analysis attack**

Standaert, F.-X.; Peeters, E.; Quisquater, J.-J.;  
*Information Technology: Coding and Computing, 2005. ITCC 2005. International*  
 Volume 1, 4-6 April 2005 Page(s):562 - 567 Vol. 1  
 Digital Object Identifier 10.1109/ITCC.2005.213

[Abstract](#) | Full Text: [PDF\(160 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

6. **Power-analysis attack on an ASIC AES implementation**  
Ors, S.B.; Gurkaynak, F.; Oswald, E.; Preneel, B.;  
Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004 Conference on

Volume 2, 2004 Page(s):546 - 552 Vol.2  
Digital Object Identifier 10.1109/ITCC.2004.1286711

[Abstract](#) | Full Text: [PDF\(1547 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

7. **Design of an RSA module against power analysis attacks**

Jiang Huiping; Mao Zhigang;  
ASIC, 2003. Proceedings. 5th International Conference on  
Volume 2, 21-24 Oct. 2003 Page(s):1308 - 1311 Vol.2

[Abstract](#) | Full Text: [PDF\(284 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

8. **An on-chip signal suppression countermeasure to power analysis attack**

Ratanpal, G.B.; Williams, R.D.; Blalock, T.N.;  
Dependable and Secure Computing, IEEE Transactions on  
Volume 1, Issue 3, July-Sep 2004 Page(s):179 - 189  
Digital Object Identifier 10.1109/TDSC.2004.25

[Abstract](#) | Full Text: [PDF\(872 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

9. **Enhancing Power Analysis Attacks against Cryptographic Devices**

Bucci, M.; Giancane, L.; Luzzi, R.; Scotti, G.; Trifiletti, A.;  
Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International  
21-24 May 2006 Page(s):2905 - 2908  
Digital Object Identifier 10.1109/ISCAS.2006.1693232

[Abstract](#) | Full Text: [PDF\(2224 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

10. **A data-driven approach for embedded security**

Saputra, H.; Ozturk, O.; Vijaykrishnan, N.; Kandemir, M.; Brooks, R.;  
VLSI, 2005. Proceedings. IEEE Computer Society Annual Symposium on  
11-12 May 2005 Page(s):104 - 109  
Digital Object Identifier 10.1109/ISVLSI.2005.4

[Abstract](#) | Full Text: [PDF\(136 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

11. **Power-balanced self checking circuits for cryptographic chips**

Murphy, J.; Bystrov, A.; Yakovlev, A.;  
On-Line Testing Symposium, 2005. IOLTS 2005. 11th IEEE International  
6-8 July 2005 Page(s):157 - 162  
Digital Object Identifier 10.1109/IOLTS.2005.56

[Abstract](#) | Full Text: [PDF\(168 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

12. **AES-based cryptographic and biometric security coprocessor IC in 0.18-  
resistant to side-channel power analysis attacks**

Tiri, K.; Hwang, D.D.; Hodjat, A.; Bo-Cheng Lai; Shenglin Yang; Schaumont, P.  
VLSI Circuits, 2005. Digest of Technical Papers. 2005 Symposium on  
16-18 June 2005 Page(s):216 - 219  
Digital Object Identifier 10.1109/VLSIC.2005.1469370

[Abstract](#) | [Full Text: PDF\(843 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

13. A countermeasure for EM attack of a wireless PDA

Gebotys, C.H.; Tiu, C.C.; Chen, X.;

Information Technology: Coding and Computing, 2005. ITCC 2005. International Volume 1, 4-6 April 2005 Page(s):544 - 549 Vol. 1  
Digital Object Identifier 10.1109/ITCC.2005.6

[Abstract](#) | [Full Text: PDF\(192 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

14. A VLSI design flow for secure side-channel attack resistant ICs

Tiri, K.; Verbauwheide, I.;

Design, Automation and Test in Europe, 2005. Proceedings 2005 Page(s):58 - 63 Vol. 3  
Digital Object Identifier 10.1109/DATE.2005.44

[Abstract](#) | [Full Text: PDF\(296 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

15. Current flattening in software and hardware for security applications

Muresan, R.; Gebotys, C.;

Hardware/Software Codesign and System Synthesis, 2004. CODES + ISSS 2004 Conference on 2004 Page(s):218 - 223

[Abstract](#) | [Full Text: PDF\(540 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

16. A multiple power analysis breaks the advanced version of the randomize subtraction chains countermeasure against side channel attacks

Okeya, K.; Sakurai, K.;

Information Theory Workshop, 2003. Proceedings. 2003 IEEE 31 March-4 April 2003 Page(s):175 - 178

[Abstract](#) | [Full Text: PDF\(555 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

17. Design and analysis of dual-rail circuits for security applications

Sokolov, D.; Murphy, J.; Bystrov, A.; Yakovlev, A.;  
Computers, IEEE Transactions on

Volume 54, Issue 4, April 2005 Page(s):449 - 460  
Digital Object Identifier 10.1109/TC.2005.61

[Abstract](#) | [Full Text: PDF\(1272 KB\)](#) [IEEE JNL](#)  
[Rights and Permissions](#)

18. Power Attacks on Secure Hardware Based on Early Propagation of Data

Kulikowski, K.J.; Karpovsky, M.G.; Taubin, A.;

On-Line Testing Symposium, 2006. IOLTS 2006. 12th IEEE International 10-12 July 2006 Page(s):131 - 138  
Digital Object Identifier 10.1109/IOLTS.2006.49

[Abstract](#) | [Full Text: PDF\(352 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

19. Security wrappers and power analysis for SoC technology

Gebotys, C.H.; Zhang, Y.;

Hardware/Software Codesign and System Synthesis, 2003. First IEEE/ACM/IF Conference on  
1-3 Oct. 2003 Page(s):162 - 167

[Abstract](#) | [Full Text: PDF\(512 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)

□ 20. **An investigation into the security of self-timed circuits**  
Yu, Z.C.; Furber, S.B.; Plana, L.A.;  
Asynchronous Circuits and Systems, 2003. Proceedings. Ninth International S  
12-15 May 2003 Page(s):206 - 215  
Digital Object Identifier 10.1109/ASYNC.2003.1199180  
[Abstract](#) | Full Text: [PDF\(702 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

□ 21. **A comparative analysis of logic styles for secure IC's against DPA attack**  
Sundstrom, J.; Alvandpour, A.;  
NORCHIP Conference, 2005. 23rd  
21-22 Nov. 2005 Page(s):297 - 300  
Digital Object Identifier 10.1109/NORCHP.2005.1597048  
[Abstract](#) | Full Text: [PDF\(344 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

□ 22. **A side-channel leakage free coprocessor IC in 0.18/spl mu/m CMOS for e based cryptographic and biometric processing**  
Tiri, K.; Hwang, D.; Hodjat, A.; Lai, B.; Yang, S.; Schaumont, P.; Verbauwheide  
Design Automation Conference, 2005. Proceedings. 42nd  
13-17 June 2005 Page(s):222 - 227  
[Abstract](#) | Full Text: [PDF\(404 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

□ 23. **Masking the energy behavior of DES encryption [smart cards]**  
Saputra, H.; Vijaykrishnan, N.; Kandemir, M.; Irwin, M.J.; Brooks, R.; Kim, S.;  
Design, Automation and Test in Europe Conference and Exhibition, 2003  
2003 Page(s):84 - 89  
Digital Object Identifier 10.1109/DATE.2003.1253591  
[Abstract](#) | Full Text: [PDF\(390 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

□ 24. **Security-driven exploration of cryptography in DSP cores**  
Gebotys, C.H.;  
System Synthesis, 2002. 15th International Symposium on  
2002 Page(s):80 - 85  
[Abstract](#) | Full Text: [PDF\(503 KB\)](#) IEEE CNF  
[Rights and Permissions](#)